

Instructional Scenario

Spotting Insecure Software Design



Course/Duty Area: Cybersecurity Fundamentals/Programming as a Component of Cybersecurity

Estimated Time Required: 3 hours

Scenario:

Your school district is launching a Help Portal through which students can request password resets and submit help tech tickets. The district hired a contractor to build the portal quickly, and, as a tech intern, you have been asked to review a short security report that describes how the system was designed. You notice that some of the design choices and coding practices might not follow secure coding best practices, even though the system appears to be working. Your job is to read the descriptions of how the portal handles logins, passwords, and error messages, then identify which parts follow secure coding best practices and which parts could create security risks.

Big Question:

How can insecure coding and design choices put user data and systems at risk, even when the program seems to work correctly?

Focused Questions:

1. Which parts of the design follow secure coding best practices, and which parts do not?
2. How do choices about error messages, password rules, and data storage affect security?
3. How can attackers take advantage of insecure coding practices?

Student Project or Outcome:

Students will complete an analysis project where they will act as security reviewers for a new school tech system. Their job will be to evaluate whether the system's design follows secure coding and design best practices, then explain their findings.

Project-Based Assessment:

Students will receive a short report that describes how the new student help portal will handle logins, passwords, error messages, and logging. The report will intentionally mix good and bad practices. Students will read through the report, identify which parts are secure or insecure, and then explain how each part could impact security and student privacy.

Students will create a short written report, presentation, or security review memo that includes

- a summary of the portal's main security strengths and weaknesses
- a list of at least four specific practices from the description, labeled *secure* or *insecure*, with a brief explanation for each
- a list of two or three improvement ideas for the portal.

Teacher Resources:

- [Best Practices for Secure Coding](#), Safe Computing, Information and Technology Services, University of Michigan
- [A Guide to OWASP's Secure Coding Practices Checklist](#), Code Signing Store

Scenario submitted by Walisa Sabb, North Stafford High School, Stafford County Public Schools

Artificial intelligence (ChatGPT) was used in the development of this instructional scenario.